Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2025-08-05

Generated by Acunetix

Scan of www.tnnua.edu.tw

Scan details

Scan information	
Start time	2025-08-05T17:00:01.343125+08:00
Start url	http://www.tnnua.edu.tw
Host	www.tnnua.edu.tw
Scan time	31 minutes, 14 seconds
Profile	Full Scan
Server information	nginx
Responsive	True
Server OS	Unknown
Application build	25.4.250417124

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	14
Critical	0
High	1
Medium	2
Low	4
Informational	7

Alerts summary

Insecure Transportation Security Protocol Supported (TLS 1.0)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N Base Score: 6.3 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-326

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

TLS/SSL Weak Cipher Suites

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 3.3 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310

Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Insecure Frame (External)

Classification

CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L Base Score: 1.8 Attack Vector: Network Attack Complexity: High Privileges Required: High User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: Low Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: Low
CVSS3	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:L Base Score: 5.1 Attack Vector: Network Attack Complexity: High Privileges Required: High User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: Low
CVSS2	Base Score: 4.6 Access Vector: Network_accessible Access Complexity: High Authentication: Single Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-829

Affected items	Variation
Web Server	2

Possible virtual host found

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

[Possible] Internal Path Disclosure (*nix)

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

Content Security Policy (CSP) Not Implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Generic Email Address Disclosure

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) Errors and Warnings

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Insecure Transportation Security Protocol Supported (TLS 1.1)

Classification

CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:N/SA:N Base Score: 6.3 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-326

Affected items	Variation
Web Server	1

Permissions-Policy header not implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Web Application Firewall Detected

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Alerts details

Insecure Transportation Security Protocol Supported (TLS 1.0)

Severity	**High**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.0.
Request headers

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Severity	**Medium**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org (https://hstspreload.org/)
Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server
Details
URLs where HSTS is not enabled: • https://www.tnnua.edu.tw/p/412-1000-1335.php
Request headers

```
GET /p/412-1000-1335.php?Lang=en HTTP/1.1

Referer: https://www.tnnua.edu.tw/p/17-1000.php

Cookie: PageLang=zh-tw; _counter=3653061

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

TLS/SSL Weak Cipher Suites

Severity	**Medium**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The remote host supports TLS/SSL cipher suites with weak or insecure properties.

Impact

Recommendation

Reconfigure the affected application to avoid use of weak cipher suites.

References

OWASP: TLS Cipher String Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)
OWASP: Transport Layer Protection Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)
Mozilla: TLS Cipher Suite Recommendations (https://wiki.mozilla.org/Security/Server_Side_TLS)
SSLlabs: SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2 (https://datatracker.ietf.org/doc/html/rfc9155)

Affected items

Web Server
Details
Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 443): • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA Weak TLS/SSL Cipher Suites: (offered via TLS1.1 on port 443): • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443): • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA
Request headers

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
Securing cookies with cookie prefixes (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
Cookies: HTTP State Management Mechanism (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
SameSite Updates - The Chromium Projects (https://www.chromium.org/updates/same-site)
draft-west-first-party-cookies-07: Same-site Cookies (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server
Verified vulnerability
Details

List of cookies with missing, inconsistent or contradictory properties:

- https://www.tnnua.edu.tw/app/authimg.php

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/var/file/0/1000/img/1/AboutTNNUAPPT.ppsx

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/

  Cookie was set with:

  ```
  Set-Cookie: PageLang=zh-tw; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/

  Cookie was set with:

  ```
  Set-Cookie: _counter=3653058; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
```

- https://www.tnnua.edu.tw/app/index.php

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/var/file/0/1000/plugin/mobile/pictures/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/index.php

  Cookie was set with:

  ```
  Set-Cookie: PageLang=en; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/index.php

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/var/file/0/1000/pictures/125/m/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
```

- https://www.tnnua.edu.tw/p/17-1000.php

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/p/

  Cookie was set with:

  ```
  Set-Cookie: PageLang=en; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/p/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/images/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/admin/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
```

- https://www.tnnua.edu.tw/help/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/lib/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/mrtg/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/var/file/0/1000/pictures/184/m/

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

- https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/combine-en.css

  Cookie was set with:

  ```
  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; HttpOnly; Secure
  ```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
```

- https://www.tnnua.edu.tw/index.php

  Cookie was set with:

  ```
  Set-Cookie: PageLang=zh-tw; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unex
  ```

Request headers

```
GET /app/authimg.php?Code=pxx6hRrPSDL/6/fZEo54ZMlnWkJn8z%2B/WcFBByrUpsrfkIyRNFTQuvzpLQ7R6wet
HTTP/1.1

Host: www.tnnua.edu.tw

Accept-Language: en-US

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: https://www.tnnua.edu.tw/

Accept-Encoding: gzip,deflate,br

Cookie: PageLang=en; _counter=3653061

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
```

Insecure Frame (External)

Severity	**Low**
Reported by module	/httpdata/iframe_sandbox.js

Description

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as

exceptions to these restrictions.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

Recommendation

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

References

MDN | iframe: The Inline Frame Element (https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe)
HTML Standard: iframe (https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element)
HTML 5.2: 4.7. Embedded content (https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox)

Affected items

Web Server
Verified vulnerability
Details
An iframe tag references an external resource, and no sandbox attribute is set.
Request headers

```
GET / HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

Web Server
Verified vulnerability
Details
An iframe tag references an external resource, and no sandbox attribute is set.
Request headers

```
GET / HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

Possible virtual host found

Severity	**Low**
Reported by module	/Scripts/PerServer/VirtualHost_Audit.script

Description

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

Impact

Possible sensitive information disclosure.

Recommendation

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

References

Virtual hosting (https://en.wikipedia.org/wiki/Virtual_hosting)

Affected items

Web Server
Details
Virtual host: **localhost.tnnua.edu.tw** Response: `<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/x`
Request headers

```
GET / HTTP/1.1

Host: GbkRBvsJ

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Connection: Keep-alive
```

[Possible] Internal Path Disclosure (*nix)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server
Details

Pages with paths being disclosed:

- https://www.tnnua.edu.tw/
  /var/file/0/1000/msys_1000_558425_84482.ico
- https://www.tnnua.edu.tw/index.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/17-1000.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/combine-en.css
  /var/file/0/1000/mobilestyle/47/images/fav.png
- https://www.tnnua.edu.tw/index.php
  /var/file/0/1000/msys_1000_558425_84482.ico
- https://www.tnnua.edu.tw/p/412-1000-2026.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/
  /var/file/0/1000/msys_1000_558425_84482.ico
- https://www.tnnua.edu.tw/p/412-1000-86.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/412-1000-88.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/412-1000-91.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/412-1000-92.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/app/
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/412-1000-96.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/424-1000-10-1.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/412-1000-1319.php
  /var/file/0/1000/msys_1000_558425_84482.ico
- https://www.tnnua.edu.tw/p/412-1000-1320.php
  /var/file/0/1000/msys_1000_558425_84482.ico
- https://www.tnnua.edu.tw/p/412-1000-1321.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/combine-zh-tw.css
  /var/file/style/5001/images/fav.png
- https://www.tnnua.edu.tw/p/412-1000-1322.php
  /var/file/0/1000/msys_1000_6981294_74267.ico
- https://www.tnnua.edu.tw/p/412-1000-1327.php
  /var/file/0/1000/msys_1000_6981294_74267.ico

Request headers

```
GET / HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

Content Security Policy (CSP) Not Implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Paths without CSP header: • https://www.tnnua.edu.tw/ • https://www.tnnua.edu.tw/index.php • https://www.tnnua.edu.tw/p/17-1000.php • https://www.tnnua.edu.tw/p/ • https://www.tnnua.edu.tw/admin/ • https://www.tnnua.edu.tw/p/412-1000-2026.php • https://www.tnnua.edu.tw/p/412-1000-86.php • https://www.tnnua.edu.tw/p/412-1000-88.php • https://www.tnnua.edu.tw/p/412-1000-91.php • https://www.tnnua.edu.tw/p/412-1000-92.php • https://www.tnnua.edu.tw/app/ • https://www.tnnua.edu.tw/p/412-1000-96.php • https://www.tnnua.edu.tw/p/412-1000-1767.php • https://www.tnnua.edu.tw/p/412-1000-2027.php • https://www.tnnua.edu.tw/p/412-1000-2028.php • https://www.tnnua.edu.tw/p/412-1000-3806.php • https://www.tnnua.edu.tw/p/412-1000-98.php • https://www.tnnua.edu.tw/p/424-1000-10-1.php • https://www.tnnua.edu.tw/p/412-1000-1319.php • https://www.tnnua.edu.tw/p/412-1000-1320.php • https://www.tnnua.edu.tw/p/412-1000-1321.php
Request headers

```
GET / HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

Generic Email Address Disclosure

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server
Details

Emails found:

- https://www.tnnua.edu.tw/
  em1102@tnnua.edu.tw
- https://www.tnnua.edu.tw/index.php
  em1102@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-88.php
  oia@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-88.php
  em1302@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-88.php
  em1212@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-88.php
  em1104@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/
  oia@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/
  em1302@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/
  em1212@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/
  em1104@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2059.php
  em2702@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2060.php
  em1433@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2061.php
  em1812@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2062.php
  arch@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2064.php
  applied@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2063.php
  dr2003@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2065.php
  em3115@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2066.php
  em3158@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2067.php
  em2632@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2067.php
  em1821@tnnua.edu.tw
- https://www.tnnua.edu.tw/p/412-1000-2068.php
  em1832@tnnua.edu.tw

Request headers

```
GET / HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

HTTP Strict Transport Security (HSTS) Errors and Warnings

Severity	**Informational**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

References

hstspreload.org (https://hstspreload.org/)
MDN: Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server
Details

URLs where HSTS configuration is not according to best practices:

- https://www.tnnua.edu.tw/app/index.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/ - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/index.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/17-1000.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/ - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/admin/ - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-2026.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-86.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-88.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-91.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-92.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/app/ - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-96.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-1767.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-2027.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-2028.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-3806.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-98.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/424-1000-10-1.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/p/412-1000-1319.php - max-age is less that 1 year (31536000);
- https://www.tnnua.edu.tw/app/showauthimg.php - max-age is less that 1 year (31536000);

Request headers

```
POST /app/index.php?Action=mobilelogin HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Cookie: PageLang=en; _counter=3653061

Content-Type: application/x-www-form-urlencoded

Content-Length: 323

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive



Account=4111111111111111&Login=1&Passwd=u]H[ww6KrA9F.x-
F&authcode=94102&hdCode=pxx6hRrPSDL%252F6%252FfZEo54ZMlnWkJn8z%252B%252FWcFBByrUpsrfkIyRNFTQuvzpL
Q7R6wet&refer=1&upCode=kBEtivHSY5G8iExleHxBRzvBJHYG45R2Hc1VcY0rRGWn8DE%252FWKsA5bFhtN%252Bt5vpjRb
4hzsVhRVLm4AWuao1cbu2Zaf81IOp71gd9%252FGL7dwR43c%252FNYRpQQHxzlv8%252BkMQV
```

Insecure Transportation Security Protocol Supported (TLS 1.1)

Severity	**Informational**

Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.1.
Request headers

Permissions-Policy header not implemented

Severity	**Informational**
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server

Details

Locations without Permissions-Policy header:

- https://www.tnnua.edu.tw/
- https://www.tnnua.edu.tw/app/index.php
- https://www.tnnua.edu.tw/var/file/0/1000/plugin/mobile/pictures/
- https://www.tnnua.edu.tw/index.php
- https://www.tnnua.edu.tw/var/file/0/1000/pictures/125/m/
- https://www.tnnua.edu.tw/p/17-1000.php
- https://www.tnnua.edu.tw/p/
- https://www.tnnua.edu.tw/images/
- https://www.tnnua.edu.tw/admin/
- https://www.tnnua.edu.tw/help/
- https://www.tnnua.edu.tw/lib/
- https://www.tnnua.edu.tw/mrtg/
- https://www.tnnua.edu.tw/var/file/0/1000/pictures/184/m/
- https://www.tnnua.edu.tw/plugin/mobile/style/bootstrap/fonts/
- https://www.tnnua.edu.tw/plugin/gallery/style/autoload/
- https://www.tnnua.edu.tw/plugin/mobile/style/images/
- https://www.tnnua.edu.tw/plugin/
- https://www.tnnua.edu.tw/p/412-1000-2026.php
- https://www.tnnua.edu.tw/plugin/gallery/
- https://www.tnnua.edu.tw/var/
- https://www.tnnua.edu.tw/plugin/mobile/style/bootstrap/

Request headers

```
GET / HTTP/1.1

Referer: https://www.tnnua.edu.tw/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

Web Application Firewall Detected

Severity	**Informational**
Reported by module	/Scripts/PerServer/WAF_Detection.script

Description

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

References

Web Application Firewall Detected | Invicti (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/web-application-firewall-detected/)

Affected items

Web Server
Details
Detected Imperva SecureSphere from the response body.
Request headers

```
TESTING /9777379 HTTP/1.1

Cookie: PageLang=en; _counter=3653061

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: www.tnnua.edu.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://www.tnnua.edu.tw/
https://www.tnnua.edu.tw/admin/
https://www.tnnua.edu.tw/app/
https://www.tnnua.edu.tw/app/authimg.php
https://www.tnnua.edu.tw/app/index.php
https://www.tnnua.edu.tw/app/showauthimg.php
https://www.tnnua.edu.tw/help/
https://www.tnnua.edu.tw/images/
https://www.tnnua.edu.tw/index.php
https://www.tnnua.edu.tw/lib/
https://www.tnnua.edu.tw/mrtg/
https://www.tnnua.edu.tw/p/
https://www.tnnua.edu.tw/p/17-1000.php
https://www.tnnua.edu.tw/p/412-1000-1319.php
https://www.tnnua.edu.tw/p/412-1000-1320.php
https://www.tnnua.edu.tw/p/412-1000-1321.php
https://www.tnnua.edu.tw/p/412-1000-1322.php
https://www.tnnua.edu.tw/p/412-1000-1327.php
https://www.tnnua.edu.tw/p/412-1000-1328.php
https://www.tnnua.edu.tw/p/412-1000-1329.php
https://www.tnnua.edu.tw/p/412-1000-1332.php
https://www.tnnua.edu.tw/p/412-1000-1333.php
https://www.tnnua.edu.tw/p/412-1000-1334.php
https://www.tnnua.edu.tw/p/412-1000-1335.php
https://www.tnnua.edu.tw/p/412-1000-1336.php
https://www.tnnua.edu.tw/p/412-1000-1337.php
https://www.tnnua.edu.tw/p/412-1000-1338.php
https://www.tnnua.edu.tw/p/412-1000-1339.php
https://www.tnnua.edu.tw/p/412-1000-1340.php
https://www.tnnua.edu.tw/p/412-1000-1341.php
https://www.tnnua.edu.tw/p/412-1000-1342.php
https://www.tnnua.edu.tw/p/412-1000-1343.php
https://www.tnnua.edu.tw/p/412-1000-1344.php
https://www.tnnua.edu.tw/p/412-1000-1345.php
https://www.tnnua.edu.tw/p/412-1000-1346.php
https://www.tnnua.edu.tw/p/412-1000-1347.php
https://www.tnnua.edu.tw/p/412-1000-1348.php
https://www.tnnua.edu.tw/p/412-1000-1349.php
https://www.tnnua.edu.tw/p/412-1000-1350.php
https://www.tnnua.edu.tw/p/412-1000-1767.php
https://www.tnnua.edu.tw/p/412-1000-1816.php
https://www.tnnua.edu.tw/p/412-1000-1817.php
https://www.tnnua.edu.tw/p/412-1000-2026.php
https://www.tnnua.edu.tw/p/412-1000-2027.php
https://www.tnnua.edu.tw/p/412-1000-2028.php
https://www.tnnua.edu.tw/p/412-1000-2049.php
https://www.tnnua.edu.tw/p/412-1000-2050.php
https://www.tnnua.edu.tw/p/412-1000-2051.php
https://www.tnnua.edu.tw/p/412-1000-2052.php
https://www.tnnua.edu.tw/p/412-1000-2059.php
https://www.tnnua.edu.tw/p/412-1000-2060.php
https://www.tnnua.edu.tw/p/412-1000-2061.php
https://www.tnnua.edu.tw/p/412-1000-2062.php
https://www.tnnua.edu.tw/p/412-1000-2063.php
https://www.tnnua.edu.tw/p/412-1000-2064.php
https://www.tnnua.edu.tw/p/412-1000-2065.php
https://www.tnnua.edu.tw/p/412-1000-2066.php
https://www.tnnua.edu.tw/p/412-1000-2067.php
https://www.tnnua.edu.tw/p/412-1000-2068.php

https://www.tnnua.edu.tw/p/412-1000-2071.php
https://www.tnnua.edu.tw/p/412-1000-2072.php
https://www.tnnua.edu.tw/p/412-1000-3750.php
https://www.tnnua.edu.tw/p/412-1000-3751.php
https://www.tnnua.edu.tw/p/412-1000-3752.php
https://www.tnnua.edu.tw/p/412-1000-3754.php
https://www.tnnua.edu.tw/p/412-1000-3755.php
https://www.tnnua.edu.tw/p/412-1000-3756.php
https://www.tnnua.edu.tw/p/412-1000-3806.php
https://www.tnnua.edu.tw/p/412-1000-86.php
https://www.tnnua.edu.tw/p/412-1000-88.php
https://www.tnnua.edu.tw/p/412-1000-91.php
https://www.tnnua.edu.tw/p/412-1000-92.php
https://www.tnnua.edu.tw/p/412-1000-96.php
https://www.tnnua.edu.tw/p/412-1000-98.php
https://www.tnnua.edu.tw/p/424-1000-10-1.php
https://www.tnnua.edu.tw/plugin/
https://www.tnnua.edu.tw/plugin/gallery/
https://www.tnnua.edu.tw/plugin/gallery/style/
https://www.tnnua.edu.tw/plugin/gallery/style/autoload/
https://www.tnnua.edu.tw/plugin/mobile/
https://www.tnnua.edu.tw/plugin/mobile/style/
https://www.tnnua.edu.tw/plugin/mobile/style/bootstrap/
https://www.tnnua.edu.tw/plugin/mobile/style/bootstrap/fonts/
https://www.tnnua.edu.tw/plugin/mobile/style/images/
https://www.tnnua.edu.tw/robots.txt
https://www.tnnua.edu.tw/var/
https://www.tnnua.edu.tw/var/file/
https://www.tnnua.edu.tw/var/file/0/
https://www.tnnua.edu.tw/var/file/0/1000/
https://www.tnnua.edu.tw/var/file/0/1000/img/
https://www.tnnua.edu.tw/var/file/0/1000/img/1/
https://www.tnnua.edu.tw/var/file/0/1000/img/1/AboutTNNUAPPT.ppsx
https://www.tnnua.edu.tw/var/file/0/1000/img/117/
https://www.tnnua.edu.tw/var/file/0/1000/img/542/
https://www.tnnua.edu.tw/var/file/0/1000/img/543/
https://www.tnnua.edu.tw/var/file/0/1000/img/543/538217247.odt
https://www.tnnua.edu.tw/var/file/0/1000/img/544/
https://www.tnnua.edu.tw/var/file/0/1000/img/546/
https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/
https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/47/
https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/47/images/
https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/combine-en.css
https://www.tnnua.edu.tw/var/file/0/1000/mobilestyle/combine-zh-tw.css
https://www.tnnua.edu.tw/var/file/0/1000/pictures/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/125/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/125/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/175/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/175/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/184/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/184/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/195/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/195/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/545/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/545/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/664/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/664/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/775/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/775/m/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/789/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/789/m/

https://www.tnnua.edu.tw/var/file/0/1000/pictures/976/
https://www.tnnua.edu.tw/var/file/0/1000/pictures/976/m/
https://www.tnnua.edu.tw/var/file/0/1000/plugin/
https://www.tnnua.edu.tw/var/file/0/1000/plugin/mobile/
https://www.tnnua.edu.tw/var/file/0/1000/plugin/mobile/pictures/
https://www.tnnua.edu.tw/var/file/0/1000/randimg/
https://www.tnnua.edu.tw/var/file/js/
https://www.tnnua.edu.tw/var/file/js/m_20250703.js
https://www.tnnua.edu.tw/var/file/style/
https://www.tnnua.edu.tw/var/file/style/5001/
https://www.tnnua.edu.tw/var/file/style/5001/images/